UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 09-10243-MLW
	)	
RYAN HARRIS	)	

DEFENDANT'S REPLY TO GOVERNMENT'S
OPPOSITION TO RENEWED MOTION TO DISMISS

Defendant Ryan Harris respectfully replies to the Government's Opposition to his Motion to Dismiss the Superseding Indictment, in particular to its foundational argument that criminal liability can be premised on the capability of defendant's firmware.[1]

I. THE GOVERNMENT'S PREMISE, THAT A PRODUCT'S CAPABILITY SUFFICES TO ESTABLISH CRIMINAL CULPABILITY, IS UNSUPPORTED IN LAW AND FAILS TO ESTABLISH VENUE IN THIS DISTRICT

The wire fraud allegations in the Superseding Indictment rest on allegations that defendant's products were wrongfully used by customers (to obtain free internet service). These allegations reduce to the notion that a product's capability alone may support conspiracy and aiding and abetting convictions (and hence venue here). This proposition – that capability

[1] This memo addresses the flawed premise upon which the government's entire case rests. In his previous memorandum, Mr. Harris addressed a number of distinct issues, including the issue of defining the alleged conspiracy and a request for a discretionary change of venue, all of which stem, ultimately, from the government's flawed premise. Because the government does not acknowledge the breadth, novelty, and implications of its charging decisions, and proceeds as though this is an entirely run-of-the-mill case, the government's opposition does not adequately respond to the arguments that Mr. Harris made in his original memorandum. Accordingly, in this memorandum, Mr. Harris addresses the government's fundamental misunderstanding and continues to urge, but does not rehash, each of the discrete arguments he addressed in his initial memorandum.

suffices for culpability – is unrecognized in criminal law, and is a contested notion even in civil law. Yet it underlies this case, sub silentio, as is evident in the broad ranging claim that Harris conspired with all users, not merely customers, in their end-use of the products. In the Superseding Indictment, only four customers are named, and only one of them is even alleged to have communicated with Harris outside of the process of ordering products,[2] with no allegation that the communication itself encouraged wrongful use of products. It is on these spare offerings that Harris is hauled into this jurisdiction, with the government asking deference from this Court until its case unfolds. By then, however, the abuse combated by the constitutional assurance of appropriate venue will have occurred.

A.

The premise on which the present action depends – that a supplier of a product which enables wrongdoing by others may be secondarily liable for the conduct of those others – is problematic even in the civil law. In general, a seller of a product cannot be held civilly liable for the conduct of third party product users. The logic is that "[u]sually the criminal use of a product is deemed to be a supervening, intervening event that eliminates any responsibility on the part of the manufacturer." George A. Nation, Respondeat Manufacturer, 60 Baylor L. Rev. 155, 157-58 (2008); see Delahanty v. Hinckley, 564 A.2d 758, 762 (D.C. Ct. App. 1989) ("'In general no

[2] The government alleges that Harris and the two alleged co-conspirators who were TCNISO employees "communicated repeatedly online with N.H. [an alleged user of TCNISO products] about cable modem hacking." Superseding Ind. at ¶ 36. However, the indictment only specifies one such communication, alleging that N.H. discussed "hacking into . . . RoadRunner, in order to obtain free internet service" with the vice-president of TCNISO, Craig Phillips. The indictment does not identify any specific conversations between Harris and N.H. Rather, discovery discloses that N.H. initiated an internet chat with Harris, telling him that he had access to TCNISO forums and had talked to a TCNISO software developer, and asked Harris if he could be a forum moderator. Harris replied, "I don't know you," and later rebuffed him, saying "I told you, I am not looking for new [forum] moderators." Discovery, Bates No. Harris128.

liability exists in tort for harm resulting from the criminal acts of third parties, although liability for such harm sometimes may be imposed on the basis of some special relationship between the parties.'" (quoting Hall v. Ford Enterprises, Ltd., 445 A.2d 610, 611 (D.C. Ct. App. 1982))). Nor do the civil courts typically find liability based on the decision to sell or market a product that can be used for unlawful purposes. See id. at 761; Perkins v. F.I.E. Corp., 762 F.2d 1250, 1265 n.43 (5th Cir. 1985) ("The marketing of a handgun is not dangerous in and of itself, and when injury occurs, it is not the direct result of the sale itself, but rather the result of actions taken by a third party."); McCarthy v. Olin Corp., 119 F.3d 148, 157 (2nd Cir. 1997) (dismissing civil suit filed by crime victims against maker of hollow point bullets and noting that manufacturer "was under no legal duty to prevent criminal misuse of its product").

The idea that intervening criminal conduct by a user prevents civil liability for the manufacturer is long-established. Oliver Wendell Holmes confronted the question "why is not a man who sells fire-arms answerable for assaults committed with pistols bought of him, since he must be taken to know the probability that, sooner or later, some one will buy a pistol of him for some unlawful end?" Holmes, Privilege, Malice, and Intent, 8 Harv. L. Rev. 1, 10 (1894). Holmes explained that generally, such vicarious liability does not exist, even in civil cases, because "every one has a right to rely upon his fellow-men acting lawfully, and, therefore, is not answerable for himself acting upon the assumption that they will do so, however improbable it may be." Id. (emphasis added).[3]

[3] Holmes went on to state the following rule: "[W]here it is sought to make a man answerable for damage, and the act of a third person is nearer in time than the defendant's to the harm, if the third person's act was lawful, it stands like the workings of nature, and the question is whether it reasonably was to be anticipated or looked out for; but if the third person's act was unlawful, the defendant must be shown to have intended the act, or at least to have expected it, and to have intended consequences which could not happen without the act." Holmes, Privilege,

Courts have been extremely circumspect about extending civil liability past this boundary. An exception is Rice v. Paladin Enterprises, Inc., 128 F.3d 233 (4th Cir. 1997), where the Fourth Circuit determined that a publisher of book entitled Hit Man: A Technical Manual for Independent Contractors could be held civilly liability for aiding and abetting criminal conduct where "a reasonable jury clearly could conclude from the stipulations of the parties, and, apart from the stipulations, from the text of Hit Man itself and the other facts of record, that [the publisher] aided and abetted in Perry's triple murder by providing detailed instructions on the techniques of murder and murder for hire with the specific intent of aiding and abetting the commission of these violent crimes. Id. at 255 (emphasis added). It is notable that the Fourth Circuit reached this conclusion only after determining that the publisher had specific intent to aid the criminal conduct. Other civil cases have gone the other way. See Herceg v. Hustler Magazine, Inc., 814 F.2d 1017 (5th Cir. 1987) (holding that publisher of article describing how to perform autoerotic asphyxia could not be civilly liable for inciting the death of a teenager).

In any event, no one contended that Hit Man's publisher might be criminally prosecuted as an accessory to murder.

B.

The pleadings here seek to import a standard, controversial in the civil law, into the criminal law. Conduct insufficient for civil liability is charged under the wire fraud statute, a

---

Malice, and Intent, 8 Harv. L. Rev. at 11-12. Even assuming that this weaker formulation of the rule is correct and proof of expectation of the unlawful act can form the basis for liability, Holmes was confronting the extent of civil liability, not the potential reach of criminal culpability. There are indications, however, that mere expectation of criminal misconduct cannot form the basis for civil liability. In a related context, Prosser & Keeton explained that "Where there is a malicious or criminal act, the original actor might be free to say, even if anticipating the misconduct, that it was not the actor's concern." Prosser & Keeton on Torts § 44, at 318 (5th ed. 1984).

statute whose breadth caused the First Circuit to warn that it must not "be used to prosecute kinds of behavior that, albeit offensive to the morals or aesthetics of federal prosecutors, cannot reasonably be expected by the instigators to form the basis of a federal felony." United States v. Czubinski, 106 F.3d 1069, 1079 (1st Cir. 1997). This use of the wire fraud statute to pioneer a novel form of criminal liability for product manufacturers drives the argument, developed in Harris' original memorandum, that the prosecution is vague and overreaching. Def't Memo. Section IV.

The government's core allegation is that the TCNISO's firmware was "inherently susceptible to illegal use." Gov't Opp. at 11. It claims that "[c]ourts have repeatedly held that where, as here, the very nature of the products or services supplied are inherently suspicious, a jury can infer that the supplier had the requisite criminal intent." Id. In fact, the "inherently suspicious" standard does not exist in this context.[4] Instead, the relevant cases draw a distinction between legally restricted products and unrestricted products. These cases lead to the conclusion that the character of an unrestricted product cannot, alone, support the conviction of a product distributor based on a customer's conduct, even if the distributor knew about the unlawful use.

In a case involving the sale of unrestricted commodities, namely quantities of yeast, sugar, and packing cans sold to illegal alcohol distillers, the Supreme Court held that an individual who supplies an unrestricted commodity is not liable for the use by a customer even when the seller knows of the use. See United States v. Falcone, 311 U.S. 205 (1940). The Court reinforced this holding in Direct Sales Co. v. United States, 319 U.S. 703, 711 (1943), in which it confronted the

[4] A Westlaw search for this term turns up cases about drug courier profiles, Terry stops, insider trading, and discriminatory employment decisions, but none discussing how or why a product manufacturer can be held criminally liable for the conduct of product users.

secondary liability of a seller of legally restricted products. In Direct Sales, the defendant company, a registered drug wholesaler, was convicted of conspiracy to violate the narcotics laws upon a showing that the corporation "sold morphine sulphate to Dr. Tate in such quantities, so frequently, and over so long a period it must have known he could not dispense the amounts received in lawful practice and was therefore distributing the drug illegally." Id. at 705. The Court noted that in contrast with Falcone, these were not "articles of free commerce," but were "restricted commodities, incapable of further legal use except by compliance with rigid regulations." Id. at 711. The Court held that the seller of a restricted product may be liable where there were repeated sales of the restricted commodity and profits from the repeated sales. This liability is distinguished from that of the seller of an unrestricted commodity, like the defendant in Falcone.

Here, there is no allegation that Harris knew when or against whom the product was actually used by the lone customer with whom he is alleged to have communicated. As for the remaining three named customers, there is no allegation that Harris even knew whether the products were used, and this proof is particularly absent regarding allegations of criminal liability for all users, not simply customers. Even if the facts were otherwise, however, under Falcone and Direct Sales, actual knowledge of misuse would not suffice for criminal culpability. Id. at 709. ("[O]ne does not become a party to a conspiracy by aiding and abetting it, through sales of supplies or otherwise, unless he knows of the conspiracy; and the inference of such knowledge cannot be drawn merely from knowledge the buyer will use the goods illegally.").

C.

The government tacitly recognizes, in the face of Falcone and Direct Sales, the inadequacy of its theory that Harris is culpable because the firmware he distributed was

susceptible to illegal use. In its brief, the government almost immediately, and without benefit of case law, shifts from the assertion that the firmware was capable of illegal uses to the assertions that the firmware constituted a "criminal tool," and that "sellers of criminal tools can be criminally liable." Gov't Opp. at 10. The government apparently argues that the firmware is malum in se, inherently bad, and then piles on the unsupported assertion that someone who sells something inherently bad must be committing a crime. But criminal law requires something to be malum prohibitum, or bad because Congress said so. Cf. Liparota v. United States, 471 U.S. 419, 424 (1985) ("The definition of the elements of a criminal offense is entrusted to the legislature, particularly in the case of federal crimes, which are solely creatures of statute."). In any event, the argument is mere ipse dixit and does not acknowledge cases which, in the civil arena, hold the opposite. A conspicuous example is the Second Circuit's ruling in McCarthy, in a suit by victims of the notorious 1993 Long Island Railroad shootings, that the manufacturer of "Black Talon" bullets had no duty not to sell or market a legal, non-defective product. 119 F.3d at 157. In the civil context, product sellers have no duty to refrain from manufacturing or marketing lawful products because of their potential to cause harm. See Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442, 456 (1984) (finding VCR manufacturer not liable for copyright infringement by product users because VCR had commercially significant non-infringing uses).

Moreover, the government does not allege that theft of cable service was the sole use of the firmware. Nor could it. The company's cable modem functioned, as does any cable modem, to link to the internet. The firmware could also be used to circumvent cable company controls,[5]

[5] The grievances of ISP customers are many. For example, ISPs aggressively throttle traffic and web speed of their customers. For example, the FCC sought to bring a large ISP to heel over its practice of blocking peer-to-peer connections, which in the view of the FCC amounted to blocking access to web content: "the evidence . . . shows that Comcast selectively

either web speed or web identifiers, at most a violation of terms of service,[6] not wire fraud. The government focuses on the fact that Harris's firmware allegedly permitted theft of MAC addresses, but does not acknowledge the fact that this conduct is not unlawful. MAC addresses are not legally protected, meaning that harvesting MACs, and making and distributing a product with that capability, is not unlawful. See Memorandum in Support of Dismissal at 27-28. A MAC is simply a number identifying a modem, just like a VIN is a number that identifies a vehicle; it is not private and is not legally protected. Large internet companies regularly harvest MACs for a host of reasons.[7] In its reply, the government ignored this reality, as well as the absence of any legal prohibition, merely renewing its unsupported claim that a harvesting capability is unlawful. Internet giants such as Google might take exception.

The government further alleges that Harris published a book "Hacking the Cable Modem," under a nom de plume. It argues at page 16 of its Opposition that Harris "went to

---

targeted and terminated the upload connections of its customers' peer-to-peer applications and that this conduct significantly impeded consumers' ability to access the content and use the applications of their choice." In the Matters of Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation, 23 F.C.C.R. 13028, 13054 (2008), rev'd on jurisdictional grounds by Comcast v. FCC, 600 F.3d 642 (D.C. Cir. 2010).

[6] Even intentionally breaching a terms of service agreement cannot be the basis for criminal liability. See United States v. Drew, 259 F.R.D. 449, 466-67 (C.D. Cal. 2009) (holding that intentional violation of MySpace's terms of service could not form basis for conviction under 18 U.S.C. § 1030(a)(2)(C)).

[7] In fact, discovery reveals that while investigating N.H.'s conduct, the FBI used a program called Network Stumbler in order to detect wireless networks in a given area. See Discovery, Bates No. Harris1411-12, Harris1517-18. The FBI used this program on a normal laptop computer running a publicly available Windows operating system. This program detected wireless networks and revealed the MAC addresses of the associated modems to the FBI agent running the program. It appears that the FBI did not have a warrant authorizing the use of this program to reveal MAC addresses.

significant lengths to hide his identity," including publishing his book using an "alias," careless of the fact that Harris' name, picture, and the particulars of his personal life, appear in the book.[8]

The government would presumably concede that it is entirely lawful for Harris to publish information about a system's vulnerabilities (even if that information enables third parties to accomplish undesirable feats).[9] It must similarly concede, and has cited no caselaw to the contrary, that it is entirely lawful for Harris to sell a tool that can exploit vulnerabilities. Certainly, commercial America behaves as if the sale of tools which may be used in unlawful ways (e.g., radar detectors, burglarious tools, hacking software) does not create criminal culpability. A standard framed to ensnare Harris, along the lines of "a seller of a legal product capable of bad applications aids and conspires with endusers in their foreseeable bad conduct," ensnares many in the marketplace. With stakes so great, one might expect the government to acknowledge the breadth of its ambitions here, and not behave as if this case was a routine application of known legal standards.

---

[8] The government contends that "Harris's efforts to hide his identity further support the inference that he shared the users' criminal intent." Gov't. Opp. at Memo at 16. The government should examine the copyright page ("Copyright © 2006 by Ryan Harris") and the personal information and photograph at the rear of the book.

[9] For example, bomb making instructions have been available on the internet for decades. In a report issued in 1997, the Department of Justice concluded that "[t]he First Amendment would impose substantial constraints on any attempt to proscribe indiscriminately the dissemination of bombmaking information." DOJ, Report on the Availability of Bombmaking Information (April 1997) available at http://www.derechos.org/human-rights/speech/bomb.html. "The government generally may not . . . punish persons either for advocating lawless action or for disseminating truthful information - including information that would be dangerous if used - that such persons have obtained lawfully." Id.; see also Bryan J. Yeazel, Note, Bomb-Making Manuals on the Internet: Maneuvering a Solution Through First Amendment Jurisprudence, 16 Notre Dame J.L. Ethics & Pub. Pol'y 279, 284 (2002); Herceg, 814 F.2d at 1017 (holding that publisher of article describing how to perform autoerotic asphyxia could not be held civilly liable for inciting the death of a teenager).

II. THE RADICAL PROPOSITION THAT A SELLER OF LAWFUL FIRMWARE MIGHT BE CRIMINALLY LIABLE FOR "PRODUCT CAPABILITY" OR FOR THE ACTIONS OF PRODUCT ENDUSERS WOULD SEND SHUDDERS THROUGH THE HIGH TECH INDUSTRY.

Much of modern communications technology tests legal boundaries. This has been true historically; printing presses certainly, and photocopiers more recently, permitted piracy. The VCR narrowly escaped being declared contraband in 1984. See Sony Corp., 464 U.S. at 456. Today, computers piggyback onto open wireless networks in bars and hotels. In other words, they intrude in and exploit vulnerable networks to provide maximum coverage for users. Each such exploitation is a computer trespass, entirely foreseeable to the program designer.

Under the government's theory here, the manufacturer of a wireless-signal-seeking device, having manufactured a product "susceptible" to illegal use, would be criminally liable for the intrusion. But the list of such products goes far beyond the world of computer technology. Products susceptible of misuse would include DVD burners, radar detectors, radar jammers, handguns, assault weapons, ammunition such as hollow point or Teflon coated bullets, flash suppressors, large capacity magazines, digital file sharing software, and alcoholic beverages. See Nation, Respondeat Manufacturer, 60 Baylor L. Rev. at 169 (listing products that author believes should subject the manufacturer to civil liability based on conduct of product users because the product "increases the risk of harm to the public from criminal conduct above the level of such risk–the background level–that would otherwise exist without the availability of the product").

As for products which can test or compromise security systems (as is alleged against Harris), one might look at a widely used software, Metasploit, distributed by a Boston-based

company. A book describing the software, Metasploit: The Penetration Tester's Guide published by No Starch Press which also offered Harris' book,[10] explains how to use Metasploit to:

> - Find exploits in unmaintained, misconfigured, and unpatched systems
> - Perform reconnaissance and find valuable information about a target
> - Bypass antivirus technologies and circumvent security controls
>
> ***
>
> - Use the Meterpreter shell to launch attacks from inside a network.

No Starch Press, Review of Metasploit: The Penetration Tester's Guide, July 7, 2011, available at http://nostarch.com/releases/metasploit_pr.html. The firmware permits users to "secure their own network or to put someone else's to the test," id., that is, to hack into secured networks. Computer attackers rely on tools such as Metasploit (and CORE IMPACT and Immunity CANVAS)[11] as powerful aids for launching network attacks. With such tools, an attacker does not have to create custom exploit code or scour the Internet to find code to exploit a hole.

Unlike Harris, who published a book and software exposing exploits regarding cable modems, Metasploit's designers did far more: they created "the Swiss army knife used by hackers," see Fred Martin, "Students Delve Into Metasploit," May 16, 2011, available at http://blog.uml.edu/cs/2011/05/fu_metasploit_presentations.html, a tool at the core of computer hacks world-wide with more than one million downloads yearly and a blog that provides customer support and tutorials for its users. See "Learn More about the Metasploit Project," available at http://metasploit.com/learn-more/; Rapid7 Community, Metasploit, available at

---

[10] No Starch Press publishes books focused on "open source, security, hacking, programming, alternative operating systems." See http://www.nostarch.com.

[11] See www.coreserurity.com ("By replicating actual threats across the enterprise, our solutions reveal where and how attacks can access your most important information."); http://immunityinc.com/products-canvas.shtml (CANVAS "makes available hundreds of exploits").

https://community.rapid7.com/community/metasploit?view=blog. The software is owned, and the blog is maintained, by Rapid7, a Boston-based security company which also owns "John the Ripper," a popular password cracking tool. Rapid7 maintains that its tools are to be used for security testing only, not for illegal hacking activity.[12] Metasploit, "Penetration Testing Basics," available at http://www.metasploit.com/learn-more/penetration-testing-basics/ ("Let's make one thing crystal clear: Penetration testing requires that you get permission from the person who owns the system. Otherwise, you would be hacking the system, which is illegal in most countries – and trust me, you don't look good in an orange jump suit."). Harris affirmed a similar purpose: "[c]able networks around the world are often misconfigured and highly vulnerable, and this book will expose countless exploits and hacking techniques . . . [providing] a wake-up call for every cable operator to implement all of the DOCSIS security features." Harris, Hacking the Cable Modem at xxiv.

Surely the government is not advocating prosecution of Rapid7 for its firmware, but it is a mystery how it distinguishes Harris' prosecution. One could substitute Rapid7's name for Harris' in the indictment and find a tidy fit.

Moreover, the conspiracy charged here is boundless in scope, linking the seller with all users. Unlike the conventional conspiracy, where a central actor is linked to others who in turn are linked to each other (a rim and spokes conspiracy), here there is no rim and the government contends it needs none. The conspiracy is boundless (the government claims intrusions into no fewer than 22 internet service providers, and declined particulars about users and use becase "we

[12] These firms collect security exploits and compress them into a single tool, thereby diminishing the skills needed for aspiring hackers worldwide. Widespread broadcast of the latest hacking exploits has the in terrorem effect of stimulating sales of anti-hacking products.

cannot identify the dates of all of these accesses" Discovery Letter, May 17, 2010). Proof at trial would mimic a contributory liability case, heavy on product capability and light on specific conduct, with the government insisting that Harris surely knew that he was selling a product certain to be used for theft of service. Whether this would suffice for a civil case, this surely plows new ground criminally. Using the Metasploit example again, its creators surely knew they were unleashing a hacking tool; if the government can find a few bad users, can it package a criminal case resting on product capability and vague testimony about the universe of potential bad users? And what about gun manufacturers who have escaped civil liability for end users, can they face criminal charges brought by an ambitious government?

Making the creator of a tool, rather than those who do illegal things with the tool, criminally culpable is a true Pandora's box which courts have declined to open on the civil side of the law. Or, to indulge another metaphor from antiquity, the notion that criminal culpability emerges whole from the wire fraud statute recalls Athena emerging full-blown from the head of Zeus.[13]

---

[13] I give you proof that all I say is true.
The father can father forth without a mother.
Here she stands, our living witness.
Child sprung full-blown from Olympian Zeus,
never bred in the darkness of the womb
but such a stock no goddess could conceive!
Aeschylus' Eumenides.

III. PRETRIAL RESOLUTION OF THESE NOVEL ISSUES IS NECESSARY TO ASSURE THE CONSTITUTIONAL RIGHT TO PROPER VENUE

The government fails to acknowledge the groundbreaking character of this prosecution.[14] One reason, certainly, is that such an acknowledgment would add to its burden in justifying prosecution in a far-off jurisdiction.

If pressed to admit the scope of its proof, the government would fairly acknowledge that Harris had no contact with three of four customers, and that he bore hostility toward the fourth (see footnote 2, supra), and further, that the government's case rests fundamentally and entirely on the alleged capability of the firmware and on actions of product purchasers and end users. No known caselaw supports a conviction on such grounds; no sound reason supports venue in this District, with its ordeal of trial in a distant court, on a legal chimera.

Yet the government invokes the criminal rule discouraging pretrial contest. But this is not the usual drug or gun case, where the template for prosecution is well established. Rule 12 "encourage[s] district courts to entertain and dispose of pretrial criminal motions before trial if they are capable of determination without trial of the general issues." United States v. Levin, 973 F.2d 463, 467 (6th Cir. 1992). In Levin, the district court concluded, at the Rule 12 hearing on defendants' motion to dismiss, that the government could prove neither criminal activity nor the requisite criminal intent, and dismissed the indictment. Id. at 469. Similarly, in United States v. Hall, 20 F.3d 1084, 1087-88 (10th Cir. 1994) and United States v. Risk, 843 F.2d 1059, 1061 (7th Cir. 1988), courts examined pretrial the sufficiency of proof in support of an indictment, and

[14]A similar effort, filed in the Southern District of New York on January 28, 2010, United States v. Matthew Delorey, 10 Cr. 00682, was abandoned. In Delorey, the government charged a supplier of modified cable modems with wire fraud, but dismissed the charge in favor of a plea to a misdemeanor of unlawful access under 18 U.S.C. § 1030(a)(6).

proceeded to dismiss indictments. In Hall, the court dismissed pretrial a charge of using a firearm in relation to a drug trafficking crime where police found the gun in a bedroom closet. In Risk, the court dismissed pretrial charges of currency transaction irregularities for insufficiency of evidence. See also United States v. Brown, 925 F.2d 1301, 1303-04, 1309 (10th Cir. 1991) (affirming pretrial dismissal of charges under 18 U.S.C. § 2314 and § 2315).

In United States v. O'Neill, Abisi, Palmisciano, et al., Criminal No. 93-10049-REK, Judge Keeton required the government to show, through admissible evidence, how charges of marijuana conspiracy against specific defendants fell within a statute of limitations although the indictment on its face alleged that the conspiracy extended to the disputed time. The likely reasons underlying Judge Keeton's order were efficiency and fairness – there was no reason to subject a defendant to trial, and to commit the resources of the court, if there might be insufficient proof of a critical element. The government complied with Judge Keeton's order, and, when the evidence presented showed that the conspiracy charge against certain defendants was time-barred, the government acquiesced in the court's dismissal of those defendants.

Harris submits that it is prudent to proceed as Judge Keeton did in O'Neill: to require the government to show through admissible evidence and relevant caselaw how Harris can be criminally responsible for the conduct of users of the products he allegedly distributed. It makes little sense, wastes much valuable judicial time, and jeopardizes Harris' constitutional rights to a proper venue to delay such scrutiny until the conclusion of a lengthy trial.

IV. IF THIS ACTION IS NOT DISMISSED, VENUE SHOULD BE CHANGED

Harris has contested venue in this District, and has alternatively asked for a discretionary change of venue to the Eastern District of California. The government disputes venue in that

district, despite having disclosed that it plans to indict Harris in that district for tax matters arising from the conduct at issue here. Harris yields to the government's venue election in the tax matter, wishing to avoid multi-district prosecution (which the government apparently favors), and because the Eastern District of California is closer to his current domicile (Redmond, Oregon). Otherwise, venue lawfully lies in the Southern District of California, where TCNISO had its place of business, not in this District.

CONCLUSION

For the foregoing reasons, Harris asks this Court to dismiss the indictment against him. In the alternative, Harris moves to transfer the case to the United States District Court for the Eastern District of California.

RYAN HARRIS
By his attorney,

/s/ Charles P. McGinty

Charles P. McGinty
B.B.O. #333480
Federal Defender Office
51 Sleeper Street
Boston, MA 02210
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on October 17, 2011.

/s/ Charles P. McGinty

Charles P. McGinty